UDC 004.056.5:004.032.6 **D.G. Kodlubovskyi, O.G. Oksiiuk, T.O. Pentsak**

DATA HIDING IN IMAGES USING COMBINED STEGANOGRAPHY AND CRYPTOGRAPHY

Nowadays, cyberspace security became very important all over the world. Cryptography and steganography - the art of transforming the code or the plain text into either the encrypted code or a pictures format, as used by the steganography feature, is the matter of great deal in the modern world ruler ―security. Combined they could make our message super hidden and attacker should waste a lot of time to know message. In this article we discuss the action and power of cryptography and steganography, its secured performance, hence data security.

Keywords:cryptography, steganography, stego-image, threshold value, method based on block divides, stegano coder, stegano system, JPEG-steganography, pseudo-random sequence generator (PRSG).

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. This method includes invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Cryptography defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker. The redundancy of data is also removed by compression data.

Cryptanalysis is the reverse engineering of cryptography—attempts to identify weaknesses of various cryptographic algorithms and their implementations. The encryption process is to conduct a reversible mathematical, logical, combination, and other transformations of the initial information, as a result of which the encrypted information is a chaotic set of letters, numbers and other characters and binary codes.

To encrypt information we have to use algorithm and the key transformation. Typically, the encryption algorithm for a particular method is unchanged. Initial data for the encryption algorithm are the information to be encoding, and encryption key. The key contains control information which determines the selection of transformation in certain steps of the algorithm and the size of the operands used in the implementation of the encryption algorithm [1–3].

Steganography embeds the secret message in a harmless looking cover, such as a digital image file. It is obvious that we use steganography in our life, but what is less obvious is the need for more research in the field. Simple techniques are easily detectable and there is a whole field of defeating steganography techniques called steganalysis. Stego-systems goals was to make changes not detectable by the human eye, his feature is not enough because statistical methods can detect the changes in the image even if it is not visible. Image compression also plays a role in steganography because it was found that on many occasions the result depend on the compression scheme used.

Steganography is such kind of hiding the information, that the fact of communication is taking place, by hiding message in other information. There are a lot of carrier file formats could be used, but images are the most popular, because of their frequency in internet and high-usability. In modern world exist a lot of variants of steganography techniques of hiding secret information. Some of them are more complex and all of them have respective strong and weak points. Earlier, we said, that images are the most popular cover objects used in steganography. In the domain of digital images many different image file formats exist. For these different image file formats, different steganographic algorithms exist .

There are three types of steganographic techniques used for image:

- Algorithms and transformationtechniques.
- LSB techniques.
- Masking and filtering techniques.

Let's talk about LSB-steganography.

Hiding information inside images is a popular technique nowadays. The idea is that small changes in some values (pixels, frequency components) of an analog signal would not affect the perception of the signal in a notable way. Tuning some pixels into one image could transmit several bits of additional information. The problem in the most native version of this approach is that pixel in an image, can't be safely modified.

Consequently, LSB requires that only half of the bits in an image be changed when data can be hidden in least and second least significant bits and yet the resulting stego-image which will be displayed is indistinguishable to the cover image to the human visual system. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel [1].

There are some different algorithms, which could hide information on the same level or even better.

Steganography method based on **Block** divides original image on blocks, that not intersect at all. Each block marked as twin-bit. In every block we hiding one secret bit. If twin-bit different from secret bit we have to invert LSB of the block, while twin-bit would equal to secret bit. This method allows not to change original image.

In cryptography, a mode of operation is an algorithm that uses a block cipher to provide an information service such as confidentiality or authenticity [2]. A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block [3]. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block. Method based on block is one the best methods in image steganography.

Here is the histogram that shows the difference between original image and image with hidden information:

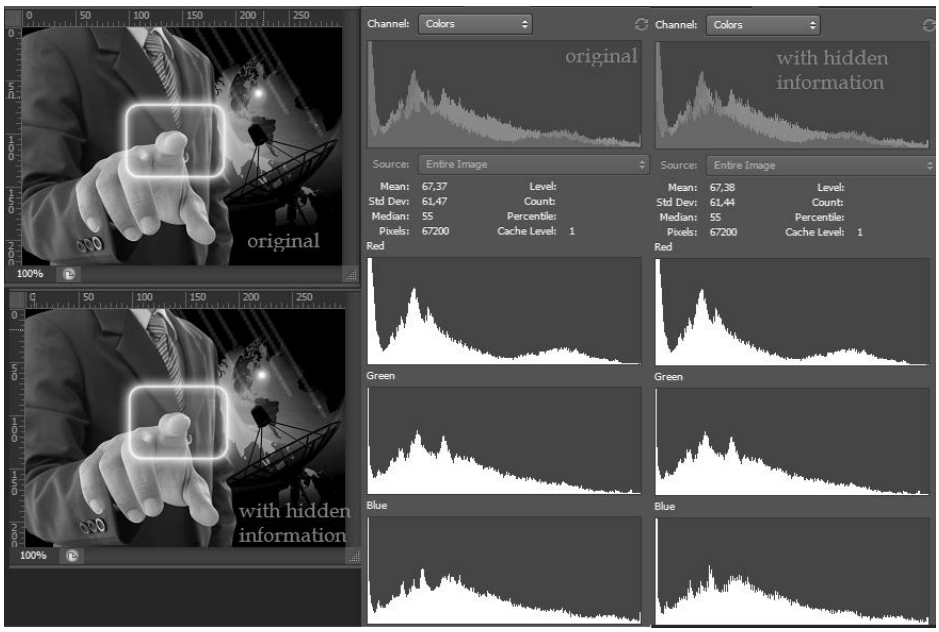

Fig. 1. Histogram that shows the difference between original image and image with hidden information

There are a lot of good methods, but showed above is one of the best, on our opinion.

We showed you the art of hiding the information – steganography , and now we will show u how to improve security of our message, by using cryptography.

Security is very important for efficient communications. Cryptography and steganography are two major branches of data security. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be found.

However, it is always a good practice to use Cryptography and Steganography together for adding multiple layers of security.

- Hiding data is better than moving it shown and encrypted.
- To hide data in image that will not attract any attention.
- In case the data is extracted, it will be encrypted and it still can't be read.

Proposed a general algorithm for such systems:

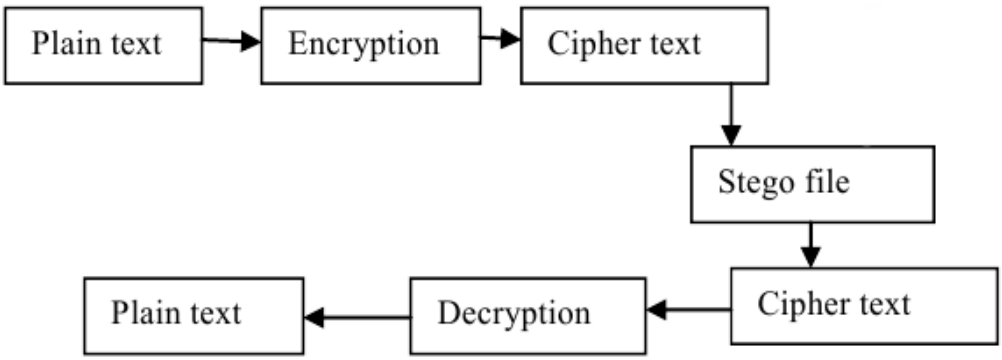

Fig.2. Proposed a general algorithm

In Ukraine this idea is poorly developed. Nevertheless, there are a number of interesting articles on this topic 1 (I.Venkata Sai Manoj, B.Tech, Hyderabad, A.P., 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 12), 2 (Khalil Challita and Hikmat Farhat, International Journal on New Computer Architectures and Their Applications, Combining Steganography and Cryptography: New Directions)]. And there are several good projects that combine steganography and cryptography. For example, STools or Steganos.

Let us show you some cryptographic algorithms we could use in combination with steganography.

A lot of stegano systems packing and retrieve messages using a key that determines the secret algorithm, which determines the procedure for making messages in the container. By analogy with the cryptography key type determines the existence of two types of stegano system [4–6].

- secret-key - one key, which determined before the start of the exchange by transmitted secure channel;
- Public-key - for packing and unpacking the message using different keys which are differs from each other so that computationally impossible to obtain a key from the other, so one of the keys (open) may be freely transmitted over insecure channel.

On this stage we are going to use pseudo-random sequence generator (PRSG). A lot of people confused about pseudo-random sequence generator and random number generator (RNG): sources of entropy is used for the accumulation of entropy and then receiving from it an initial value (initial value, seed), the required random number generators (RNG) to generate random numbers [7–10]. PRSG uses only the initial value, which implies it pseudo-randomness and always RNG generates a random number, referring to the beginning of the high-quality random value provided by various sources of entropy.

Vulnerabilities of PRSG:

- predictable relationship between numbers;

- predictable initial value generator;
- small length of the period of the generated random number sequence, after which the generator loops.

Nevertheless, we have to use pseudo-random sequence generator, because it is better for our encoder scheme.

The pseudo-random sequence generator (PRSG) bits can be used as a secret algorithm. Qualitative generator PRSG, focused on the use of information protection systems must match the certain requirements. Here is some of them:

- Cryptographic resistance – offender don't have the possibility to provide the next bit based on known by him earlier. Probability is different from 1/2. In practice, the cryptographic resistance is estimated by statistical methods.
- The good statistical properties - PRSG in its statistical properties should not differ from a truly random sequence.
- The time is used to build sequence is too big.
- Efficient of hardware and software implementation.

Let's take a look at the encoder scheme (decoder does everything the same, but in reverse order):

- Key generation. For encoder we need 2 keys: stegano and crypto secret key. Let's take the sum of the hash SHA-256 of the password entered by user. The first 16 bytes would be used for stegano key, the second - for the crypto key.
- Pre-treatment of the text (precoder). Re-take the hash-sum of crypto key and get a new 32 bytes that have to be used to encrypt data. Encrypt the data using the AES-256 algorithm.
- Starting to encode the image.
- Instead of the fifth step (quantization) of JPEG algorithm we hiding our data:
  - Size analyzator. To make the intervention in the invisible image we will conduct "visual" analysis. Every last bit of the block coefficient is inverted, and it is considered PSNR metric for the initial and modified blocks. If the metric value is less than 55 dB, the recording is not performed in this block. Because when the metric value greater than 40 dB image deemed to be practically identical to the human eye, then at 55 dB difference will definitely be noticeable to the eye.
  - Stegano way. Stegano key represented in binary form, and each block is assigned a corresponding bit binary sequence. If the result bit is one, the unit is used for recording, if zero – ignored.
  - Steganocoder. We provide LSB standard procedure for each 8x8 block: input the data in each element whose value is greater than one.
- We have continue implementation of the algorithm JPEG (lossless compression, and writing into a file).

After all we have our JPEG-image with "double"(steganography and cryptography) security.

Combination of steganography and cryptography could be very important in data security. Today we don't know all the power of steganography and the progress could be make in few decades can be that destination point, that will change our vision of information security at all. Despite of bad awareness, Steganography is a technique that hides the existence of the message, can be used to supplement encryption. By that easy way cryptography could be used in steganography methods of hiding the information into JPEG image.

References

1. Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004.

2. S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

3. Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.

4. NIST Computer Security Division's (CSD) Security Technology Group (STG) (2013). "Block cipher modes". Cryptographic Toolkit. NIST. Retrieved April 12, 2013

5. Cryptography Engineering: Design Principles and Practical Applications. Ferguson, N., Schneier, B. and Kohno, T. Indianapolis: Wiley Publishing, Inc. 2010. pp. 63, 64. ISBN 978-0-470-47424-2.

6. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (1996). Handbook of Applied Cryptography. CRC Press. pp. 228–233. ISBN 0-8493-8523-7.

7. Anderson, R.J. & Petitcolas, F.A.P., "On the limits of Steganography", IEEE Journal of selected Areas in Communications, May 1998

8. Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

9. G., Derrick, (2001), Data watermarking Steganography and watermarking of digital data, Computer Law & Security Report, 17 (2), 101-104

10. Ross J. Anderson, Fabien A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4): 474-481, May 1998. Special Issue on Copyright & Privacy Protection. ISSN 0733-8716.

Надійшла 13.05.2016 р. Рецензент: д.т.н., проф. Берзан В.П.